UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	
- v. -	No. 22 Cr. 305 (JMF)
NATHANIEL CHASTAIN,	
Defendant.	

GOVERNMENT'S MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS

DAMIAN WILLIAMS
United States Attorney
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007

Thomas Burnett
Nicolas Roos
Assistant United States Attorneys
- Of Counsel -

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

Secondary Sources

PRELIMINARY STATEMENT

Long before Nathaniel Chastain was arrested on the charges in this case, four agents from the Federal Bureau of Investigation executed a search warrant on his apartment for the limited purpose of seizing electronic devices containing evidence of the charged crimes. The agents told Chastain they were at his apartment to seize devices and had him sit, unrestrained on the bed as they efficiently went about their work, never telling Chastain he was under arrest or not free to leave, and never asking him anything about the crime under investigation. There is no allegation that the agents were anything but cordial throughout the process.

Nonetheless, Chastain moves to suppress data from a cellphone seized during the search, on the grounds that, when an agent asked him for the phone's password, the agent conducted a custodial interrogation that required a *Miranda* warning. That motion should be denied without an evidentiary hearing.

For one, the facts, even as portrayed in Chastain's affidavit, show that the agents did not need to provide a *Miranda* warning. A *Miranda* warning is necessary only if a suspect is subjected to custodial interrogation, which requires that the suspect's freedom is curtailed to the degree associated with formal arrest. When Chastain was asked for his password, however, he was not in custody: He was unrestrained, in his own apartment, and all the circumstances of the search reinforced that the agents were there to conduct a search, not to arrest him. Chastain was also not subjected to an interrogation. An agent simply asked him for is phone password, the answer to which had no realistic possibility of eliciting an incriminating statement in response.

Moreover, regardless of whether the agents should have provided a *Miranda* warning, there is no basis to suppress data seized from Chastain's cellphone. The Supreme Court and the Second Circuit have repeatedly held that suppressing non-testimonial fruits from a non-*Mirandized*

statement is inappropriate. Rather, the sole remedy is suppression of the statement. There is also no plausible argument that the alleged *Miranda* violation amounted to a Fifth Amendment violation because Chastain does not, and cannot, claim that agents used coercive measures to force him to divulge his password.

Finally, if this Court holds a hearing, which it need not, the Government expects that the evidence would confirm that the agents were not required to give Chastain a *Miranda* warning before asking for the password, and that no violation of Chastain's constitutional rights occurred. Separately, even assuming there was such a violation, the Government inevitably would have been able to extract data from Chastain's cellphone without his password, including by unlocking Chastain's cellphone using the phone's facial-recognition feature, which was activated.

BACKGROUND

The Government expects that, if the Court were to hold an evidentiary hearing, testimony from Government witnesses and other evidence would establish the following facts, among others:

On September 20, 2022, the Hon. James L. Cott issued a warrant, authorizing the Government to search Nathaniel Chastain's apartment (the "Apartment") for electronic devices and to search any seized devices for certain categories of evidence relevant to an ongoing investigation of Chastain's purchase and sale of non-fungible tokens ("NFTs"). *See* Ex. A.[1] The warrant further authorized the Government, during the execution of the warrant, to obtain from Chastain "the display of any physical biometric characteristics . . . necessary to unlock any electronic device(s)." *Id.* In the application for the warrant, an agent ("Agent-1") from the Federal

[1] For purposes of this brief, references to Chastain's motion to suppress begin with "Br." and references to exhibits attached to that motion begin with "Ex."

Bureau of Investigation ("FBI") noted that this portion of the warrant did not include the authority to "compel Chastain to provide a numeric passcode." *See* Ex. A.

Law enforcement officers executed the warrant on September 22, 2022. That morning, four FBI agents, including Agent-1, went to Chastain's apartment building to conduct the search. A typical FBI search or arrest typically involves six or more agents, but the FBI sent a smaller group due to the narrow scope of the warrant and small size of the Apartment. All four agents were wearing suits, with bulletproof vests underneath that had "FBI" written on them. The agents also wore holstered sidearms, but did not draw those weapons at any point during the operation.

The agents arrived outside the Apartment at approximately 6:48 a.m. One of the agents knocked on the door. Chastain eventually answered, and Agent-1 told him, in substance and in part, that the agents were from the FBI, that they had a warrant to search the Apartment, and that he was not under arrest. Agent-1 also told Chastain, in substance and in part, that the search warrant was for his electronic devices and that the agents would appreciate if Chastain assisted them in identifying where the devices were, so they would not need to go through everything in the Apartment. Chastain asked to see the warrant, and Agent-1 provided a copy.

Chastain handed one of the agents his iPhone (the "iPhone"), which the agents placed on a charging pad on Chastain's desk, so it would maintain power. Agent-1 told Chastain, in substance and in part, that for safety purposes, the agents wanted Chastain in a place where they could see him, so Agent-1 asked Chastain to sit on the bed. Chastain complied. Agent-1 also asked Chastain if he would provide the password to the iPhone, and Chastain provided it (the "Password"). The time that elapsed between the agents entering the Apartment and Chastain providing the passcode was less than approximately ten minutes.

The agents searched the Apartment for other electronic devices and filled out standard paperwork about the search. During that process, Chastain asked if he could speak to his lawyer. Agent-1 provided one of the agents' cellphones for Chastain to make the call, and the agents allowed Chastain to speak to his lawyer alone in the bathroom. The agents also allowed Chastain to retrieve phone numbers from the iPhone.

Ultimately, the agents seized, in addition to the iPhone, a computer, an iPad, and two ledger wallets. Before the agents left the Apartment, Agent-1 told Chastain, in substance and in part, that the agents would need to extract images from the electronic devices, which could take time. Chastain asked, in substance and in part, if he could get a new device, and Agent-1 replied that getting a new device was not a problem.

In all, the agents were in the Apartment for approximately one hour. The tone of all interactions between the agents and Chastain was conversational. Chastain never asked the agents if he was being arrested or was free to leave. And the agents never questioned Chastain about the substance of the case under investigation.

After seizing electronic devices from the Apartment, the agents brought those devices back to their office and gave the iPhone, computer, and iPad to FBI agents responsible for extracting data from those devices for a search. Using the Password, those agents extracted data from the iPhone. The agents were also able to extract data from the iPad and the computer. The latter required a thumbprint or password to open and, when the Government informed Chastain's lawyers that the warrant authorized the use of Chastain thumbprint to open devices, the attorneys

provided the password. Members of the prosecution team subsequently reviewed data from all three devices and seized data responsive to the search warrant.[2]

Finally, while the FBI used the Password to open the iPhone, the FBI has confirmed that "FaceID" was activated on the iPhone, meaning that the device could have been opened using biometric authentication.

ARGUMENT

I. The Motion Should Be Denied Because The Agents Were Not Required To Read A *Miranda* Warning Before Requesting The Password.

Chastain's motion to suppress data seized from the iPhone should be denied because the agents were not required to read him a *Miranda* warning before asking him for his Password. A *Miranda* warning is required only when a suspect is questioned as part of a custodial interrogation. But Chastain was not in "custody" when the agents were executing a targeted search for electronic devices in his apartment, and the request for his password was not "interrogation." That is clear even relying solely on the facts alleged in Chastain's affidavit, so this Court can deny his motion to suppress without holding a hearing.

A. Chastain Was Not In "Custody" When He Provided His Password.

The agents were not required to read Chastain a *Miranda* warning before speaking to him during the search of his Apartment because he was not in custody. Chastain was unhandcuffed and clearly informed that the agents had arrived to execute a warrant for electronic devices. Their

[2] Chastain's submission refers to the iPhone containing "privileged communications with counsel." Br. 2. Before members of the prosecution team reviewed data from the iPhone and other devices, the Government implemented a screening process, designed to prevent members of the prosecution team from seeing potentially privileged information. Chastain, notably, has not claimed that members of the prosecution team reviewed privileged communications.

conduct and interactions with Chastain would not have suggested to a reasonable person that Chastain was effectively subject to an arrest.

"Statements made during a custodial interrogation are generally inadmissible unless a suspect has first been advised of his or her rights." *United States v. Faux*, 828 F.3d 130, 134 (2d Cir. 2016) (citing *Miranda v. Arizona*, 384 U.S. 436, 444 (1966)). "'[C]ustody' for *Miranda* purposes is not conterminous with . . . the colloquial understanding of custody." *United States v. FNU LNU*, 653 F.3d 144, 152-53 (2d Cir. 2011). "The test for determining custody is an objective inquiry that asks (1) 'whether a reasonable person would have thought that he was free to leave the police encounter at issue' and (2) whether 'a reasonable person would have understood his freedom of action to have been curtailed to a degree associated with formal arrest.'" *Faux*, 828 F.3d at 134 (quoting *United States v. Newton*, 369 F.3d 659, 672 (2d Cir. 2004)).

The first of those questions—whether a reasonable person would have felt free to leave the encounter—is a "necessary, but not sufficient" condition, because it simply establishes that the defendant has been seized. *Id.* The "ultimate inquiry" is the second one, which focuses on "whether there is a formal arrest or restraint on freedom of movement of the degree associated with formal arrest." *United States v. Familetti*, 878 F.3d 53, 60 (2d Cir. 2017). Relevant facts include "the interrogation's duration; it's location . . . ; whether the suspect volunteered for the interview; whether the officers used restraints; whether weapons were present and especially whether they were drawn; whether the officers told the suspect he was free to leave or under suspicion; . . . [and] the nature of the questions asked." *FNU LNU*, 653 F.3d at 153.

Assessing these factors, the Second Circuit in *Faux* cautioned that "courts rarely conclude, absent a formal arrest, that a suspect question in her own home is 'in custody.'" 828 F.3d at 135-36. There, more than ten agents executed a search warrant on a suspect's home as she was

preparing to go on vacation, at the outset telling the suspect that she was "not going anywhere." *See id.* at 132-33. The agents then separated the suspect from her husband, escorted her to the dining room by holding her arm, prevented her from moving about unaccompanied, and interrogated her for two hours about facts central to the investigation, telling her that she was not under arrest only after the interview had gone on for 20 minutes. *See id.* at 132-34. Nonetheless, the Court held that the suspect was not in "custody" at any point, reasoning that the suspect was "questioned in the familiar surroundings of her home" and "was not handcuffed"; that"[t]he agents did not display their weapons" or use "physical force"; and that the suspect "was never told that she was *not* free to leave," did not "seek to end the encounter," and was questioned in a "tone" that "was largely conversational." *Id.* at 138-39.

Here, too, the facts show that Chastain was not in "custody" during the search of his Apartment, even relying solely on the facts in Chastain's affidavit. The agents efficiently executed a targeted search warrant, and no reasonable person would have understood Chastain to be restrained "to a degree associated with formal arrest" during that process. *Id.* at 137.

Chastain, like the suspect in *Faux*, was in the "familiar surroundings" of his Apartment on the morning of the search. *Id.* at 137-38; *accord Familetti*, 878 F.3d 53 at 60 ("[I]nterrogation in the familiar surroundings of one's own home is generally not deemed custodial."); Chastain Affidavit ("Aff.") ¶ 3. When the agents arrived, they knocked on the door, and Chastain voluntarily opened it. Aff. ¶ 4. There were only four agents present, which "would not, by itself, have led a reasonable person in [Chastain's] shoes to conclude that he was in custody." *Newton*, 369 F.3d at 675; Aff. ¶ 4. And lest there be any doubt about the reason for the visit, the agents promptly told Chastain why they were at the Apartment, informing him that they had a warrant to search his home and take electronic devices. Aff. ¶ 5. The agents then entered the Apartment and

told Chastain to sit on the bed, but did not force him to do so or place him in handcuffs. Aff. ¶¶ 5-6. Nothing about this entry into the Apartment would have led a reasonable person to conclude that he was under arrest. *See Faux*, 828 F.3d at 138 (noting that suspect was not handcuffed and agents did not use physical force); *Familetti*, 878 F.3d at 61("[A] certain level of restraint is acceptable in the course of a reasonable investigative detention.").

The agents' conduct during the search, as described in Chastain's affidavit, also would not have led a reasonable person to believe he was in custody akin to formal arrest. Chastain recounts that an agent asked him if a cellphone was his and asked for password for the cellphone. Aff. ¶ 7. Those questions are significant because, as the Second Circuit explained, the "nature of the questions asked," if focused on issues other than the suspect's commission of a crime, can "assure a reasonable person that he or she is not under arrest." *FNU LNU*, 653 F.3d at 154. Here, the brief, targeted questions that the agents asked Chastain would have assured a reasonable person in his shoes that the agents were, as they had represented, executing a search warrant, rather than arresting him. Indeed, while Chastain's affidavit says that he "did not feel that [he] was free to leave," Aff. ¶ 12, it notably does not say that he was so at the mercy of the police as to be in a situation akin to formal arrest. *Cf. Faux*, 828 F.3d at 135 (holding "subjective belief . . . generally does not bear on the custody analysis").

Moreover, Chastain's affidavit is noteworthy for what it does not allege. Chastain dos not claim that he asked whether he was under arrest or attempted to leave the Apartment. *See Faux*, 828 F.3d at 139 (noting that the suspect "did not seek to end the encounter"). He does not allege that the agents drew their weapons, handcuffed him, physically restrained him, threatened him, told him he was under arrest, or said he was not free to leave. *See, e.g.*, *id.* at 138-39 (finding that similar facts weighed against finding that the suspect was in custody); *FNU LNU*, 653 F.3d at 155

(same); *United States v. Valerio*, 765 F. App'x 562, 566 (2d Cir. 2019) (same). And he does not say that his interactions with the agents were anything other than respectful and conversational. *See, e.g.*, *Faux*, 828 F.3d at 139 (noting that agents did not "raise[] their voice" or "ma[ke] threats"); *Valerio*, 765 F. App'x at 566 (noting defendant was "cooperative" and "calm"). All of those factors confirm that the agents did not restrain Chastain in a manner akin to arrest.

Urging the Court to reach a contrary conclusion, the defense argues that the search of Chastain's Apartment was similar to the facts of *United States v. Butt*, No. 18 Cr. 87 (NSR), 2019 WL 479117 (S.D.N.Y. 2019). Br. 6-9. But that case, which Judge Roman noted was a "close call," *id.* at *11, bore far more hallmarks of formal arrest than the search of Chastain's apartment. In *Butt*, sixteen law enforcement officers searched the suspect's house to search for firearms. *Id.* at *2. The suspect was required to remain on his couch, as a law enforcement officer took his pedigree information and filled out "the required paperwork for an 'arrestee.'" *See id.* at *2, *12-14. While that was going on, other officer disabled a surveillance system in the suspect's house and began searching the premises, finding firearms within minutes. *Id.* Officers, within earshot of the suspect, celebrated finding the guns, which provided a basis for arresting the suspect due to his status as a felon. *Id.* at *12-14, *17. They also directly questioned the suspect about guns and ammunition; "the exact information that would be the key evidence for the crime." *Id.*

In short, the defendant in *Butt* was questioned about his criminal activity, as officers around him found evidence of that criminal activity, and as another officer was actively filling out booking paperwork. That is far different from this case, where agents searched Chastain's apartment for the limited purpose of finding electronic devices, asked only questions about that search, and gave no indication of a plan to arrest him that day.

Finally, the foregoing analysis is based solely on Chastain's affidavit, and shows why this Court can deny Chastain's motion without a hearing. If this Court were to hold a hearing, the Government expects testimony would further support that Chastain was not in "custody" when he gave the agents his password. For example, as explained above, the Government expects the evidence would show that the agents told Chastain he was not under arrest; that agents explained they were having him sit on the bed for safety reasons during the search; that agents asked Chastain to point out where devices were so they could complete the search in the quickest and least disruptive manner; and that agents allowed Chastain to retrieve phone numbers from the iPhone. The Court, however, can deny Chastain's motion based only on the affidavit he has submitted because even Chastain's recitation of the events shows he was not in "custody."

B. The Request For Chastain's Password Was Not An "Interrogation."

Separately, the agents also did not need to read Chastain a *Miranda* warning before asking for his Password because the request did not amount to an "interrogation." On the facts of this case, the agents already knew the iPhone belong to Chastain, so the request for the Password had no potential to elicit an incriminating statement.

Even when a suspect is in "custody," a *Miranda* warning is required only before the suspect is "interrogated." *Miranda*, 384 U.S. at 478. "[I]nterrogation" means "express questioning or its functional equivalent," which consists of "words or actions . . . that the police should know are reasonably likely to elicit an incriminating response." *Rhode Island v. Innis*, 446 U.S. 291, 300-01 (1980). "Not all questioning of a suspect by the police amounts to interrogation." *Familetti*, 878 F.3d at 57-58. After all, not all questions have the potential to elicit incriminating responses. *See Rosa v. McCrary*, 396 F.3d 210, 222 (2d Cir. 2005) (applying an objective test of whether officers should have known a booking question was "likely to elicit an incriminating response"). To that end, the Second Circuit has held that in-custody questioning requires a *Miranda* warning

only when that questioning has the potentially to lead to statements of an "incriminatory nature." *United States v. Rodriguez*, 356 F.3d 254, 258 (2d Cir. 2004).[3]

Here, Agent-1's request for the Password did not have the potential to, and did not, elicit an incriminating response. The only information the question could, and did, elicit was the numerical code for unlocking the phone and an implicit confirmation that Chastain knows the Password. The former has no value—it is just a series of numbers. And the latter has no value in the context of this case because it was obvious at the time of the question that the phone belonged to Chastain; it was in his Apartment, where he lived alone, and he handed it to them after being asked for his electronic devices. *See United States v. Apple MacPro Computer*, 851 F.3d 238, 248 n.7 (3d Cir. 2017) (noting, in the context of a motion to quash a subpoena, that there is a "very sound argument" that producing a password or unlocking a device is not incriminating when the suspect's ownership of a device is a "foregone conclusion"); *see also* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev.767 (2019) (arguing that unlocking a device does not infringe the privilege against self-incrimination when the Government has independent knowledge that the person knows the password). The request for the password, then, was not "interrogation" requiring a *Miranda* warning.

In arguing otherwise, Chastain notes that the password was important to accessing Chastain's iPhone, which would contain incriminating information. Br. 10. But that does not make the statement—which was just the numerical passcode—incriminating. This issue regularly arises in situations when officers request consent to search a location or device, either before giving

[3] While *Rodriguez* focused on whether the agents were "aware of the potentially incriminatory nature of the disclosure sought," the Supreme Court clarified in *FNU LNU* that the *Miranda* test is "objective," rather than focusing on the subjective awareness or intent of the officers. 653 F.3d at 152 n.7.

a *Miranda* warning or after a suspect has invoked the right to remain silent. That request, too, is likely to lead to the discovery of incriminating evidence. But courts confronting *Miranda*-based challenges to those consents consistently hold that "a request for consent to search does not constitute an interrogation within the meaning of *Miranda* insofar as it does not seek to elicit a self-incriminating statement." *United States v. St. Claire*, No. 04 Cr. 147 (LTS), 2005 WL 736236, at *4 (S.D.N.Y. Mar. 30, 2005) (collecting cases); *accord United States v. Rodriguez-Garcia*, 983 F.3d 1563, 1568 (10th Cir. 1993) ("Every federal circuit court which has addressed the *Miranda* issue . . . has reached the conclusion that a consent to search is not an incriminating statement."). By the same token, requests for passwords do not elicit incriminating *responses* just because they might lead to finding incriminating data.

Indeed, the settled line of cases holding that *Miranda* warnings are not needed when seeking consent to search require the same result for requests for passwords because the requests often go hand in hand. When officers seek consent to search an electronic device, they typically also seek consent for the password—otherwise, the consent to search could be frustrated by encryption software. This is little different than asking where to find the key to an apartment upon receiving consent to search the premises. Treating the request for consent to search and the request for a password differently for *Miranda* purposes would introduce an arbitrary distinction between the two requests, even though neither has a greater chance to elicit incriminating testimony than the other. Thus, even setting aside the issue of "custody," this Court should deny Chastain's motion to suppress because the request for his Password was not "interrogation."

II. Suppressing Data From The iPhone Is Not A Remedy For The Alleged *Miranda* And Fifth Amendment Violations.

Even assuming, *arguendo*, that the agents should have read Chastain a *Miranda* warning before asking for the Password, suppressing data seized from the iPhone would not be a legally

appropriate remedy for that error. Rather, the only available remedy is barring the Government from introducing Chastain's statement about the password in its case in chief.

To begin, the Supreme Court has long recognized a distinction between *Miranda* violations and violations of the Fifth Amendment. The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." This right "bars the introduction against a criminal defendant of out-of-court statements obtained by compulsion." *Vega v. Tekoh*, 142 S. Ct. 2095, 2101 (2022). "*Miranda* imposed a set of prophylactic rules" designed to protect defendants' Fifth Amendment rights. *Id.* at 2101-02. But the Supreme Court has consistently held "a violation of *Miranda*" is not a *per se* "violation of the Fifth Amendment right against compelled self-incrimination" because a non-*Mirandized* statement is not necessarily a compelled statement. *See id.* at 2101-03; *see also Oregon v. Elstad*, 470 U.S. 298, 306-07 (1985) (explaining that *Miranda* "sweeps more broadly than the Fifth Amendment" and excludes even "*voluntary* statements"); *United States v. Patane*, 542 U.S. 630, 634 (2004) (analyzing "unwarned but voluntary statement").

Eliding that distinction, Chastain argues that, if the agents should have read a *Miranda* warning before he gave them the Password, his Fifth Amendment rights were violated and data from the iPhone should be suppressed. Br. 12. This argument fails at multiple levels, even assuming a *Miranda* violation occurred: First, a *Miranda* violation cannot justify suppressing data from the iPhone. And second, the fact of a *Miranda* violation does not mean there was a violation of the Fifth Amendment because Chastain was not compelled to divulge his Password.

The Supreme Court and Second Circuit have repeatedly rejected the argument that "fruits" of *Miranda* violations should be suppressed. In *Michigan v. Tucker*, the Supreme Court "held that the 'fruits' of an un-*Mirandized* statement can be admitted" in evidence. *Vega*, 142 S. Ct. at 2103

(quoting *Michigan v. Tucker*, 417 U.S. 433, 450-52 n.26 (1974)). The Supreme Court reaffirmed that decision in *United States v. Patane*, rejecting the argument that "a failure to give a suspect" a *Miranda* "requires suppression of the physical fruits of the suspect's unwarned but voluntary statements." *Id.* at 633-34. Three Justices reached that conclusion by reasoning that "failure to give *Miranda* warnings does not, by itself, violate a suspect's constitutional rights," and that potential constitutional "violations occur, if at all, only upon the admission of unwarned statements into evidence at trial." *Id.* at 641-42. "Thus, . . . with respect to mere failures to warn," there is "nothing to deter" and "no reason to apply the 'fruit of the poisonous tree doctrine.'" *Id.* at 642. Two other Justices applied a balancing test, reasoning that physical evidence has "important probative value" and that introducing that evidence carries a low risk of using the accused's "incriminating statements against him." *Id.* at 644. But all five reached the same conclusion that fruits of a *Miranda* violation should not be suppressed. *See Vega*, 142 S. Ct. at 2104 n.3.

The Second Circuit, and courts in this District, have followed the holding of *Patane*, and consistently decided that "failure to give *Miranda* warnings does not require suppression of physical evidence discovered as a consequence of unwarned statements." *United States v. McCoy*, 407 F. App'x 514, 516 (2d Cir. 2010); *accord United States v. Haygood*, 157 F. App'x 448, 449 (2d Cir. 2005); *United States v. Sharma*, No. 18 Cr. 340 (LGS), 2019 WL 3802223, at *8 (S.D.N.Y. Aug. 13, 2019); *United States v. Wilson*, 914 F. Supp. 2d 550, 562 (S.D.N.Y. 2012); *United States v. Grant*, No. 07 Cr. 1119 (CM), 2008 WL 2971781, at *6-*7 (S.D.N.Y. Aug. 1, 2008).

Following Supreme Court and Second Circuit precedent leads to a straightforward result: Even if the agents had been required to read Chastain a *Miranda* warning (and they were not), their failure to do so should result in the suppression of any statements Chastain made, but not "fruits" of his un-*Mirandized* statements—including data from the iPhone. Failing to give a *Miranda*

warning was not a violation of Chastain's constitutional rights and introducing data from the iPhone at trial runs no risk of introducing Chastain's statements against him. There is, accordingly, no basis to apply the harsh remedy of suppressing probative evidence from the iPhone.

The decision in *United States v. Djibo*, upon which Chastain relies heavily, Br. 12-14, does not warrant a different result. That case arose out of vastly different circumstances. There, officers conducting a narcotics investigation stopped a suspect at the border, obtained his phone passcode, and conducted a warrantless search of the suspect's phone. 151 F. Supp. 3d 297, 299-305 (E.D.N.Y. 2015). The suspect moved to suppress the result of that search and the result of a search warrant subsequently obtained for the phone. *Id.* The Court found that the suspect was in "custody" when he provided the passcode, and the Government voluntarily suppressed evidence gathered from the pre-warrant search of the phone. *Id.* at 305-06. The Court held that the data obtained after the Government obtained a search warrant should be suppressed as a fruit of the poisonous tree, relying heavily on the warrantless search of the suspect's phone and the connection between that initial search and the subsequent warrant. *Id.* at 308-09.

Djibo and Chastain's case are fundamentally different because, here, there was never a warrantless search of the iPhone. The Agents had a warrant to search Chastain's electronic devices before they ever set foot in the Apartment or looked at any data on the iPhone. Thus, the key concern about the need to protect cellphones from unreasonable searches that animated *Djibo*—and that is reiterated in Chastain's brief, Br. 14—is not present here because a judge authorized the search before agents accessed the iPhone.

Chastain is wrong to read *Djibo* for the broader proposition that, when it comes to cellphones, the rule that physical fruits of a *Miranda* violation should not be suppressed is inapplicable. As explained above, the rule against suppression arises from *Miranda*'s purpose, not

the type of physical evidence at issue. Failure to give a *Miranda* warning is not, by itself, a constitutional violation and admitting physical evidence at trial does not risk introducing a defendant's statements against him, so there is no constitutional interest that warrant suppression. Any concerns unique to the importance of cellphones in modern life is appropriately handled by requiring that cellphones are searched only pursuant to judicially authorized warrants, as was the case here, not by ad hoc extensions of *Miranda*.

The argument that the agents violated Chastain's Fifth Amendment rights is also off base. As explained above, even assuming, *arguendo*, the agents should have given a *Miranda* warning before asking for the Password, that does not mean there was a violation of the Fifth Amendment. Rather, "the Fifth Amendment prohibits use by the prosecution in its case in chief only of *compelled* testimony," and "[v]oluntary statements remain a proper element in law enforcement." *Elstad*, 470 U.S. at 304-07. "[C]oercive police activity is a necessary predicate to the finding that a confession is not 'voluntary.'" *Colorado v. Connelly*, 479 U.S. 157, 167 (1986); *accord Elstad*, 470 U.S. at 305 (noting that the Fifth Amendment is "not concerned . . . with moral and psychological pressures to confess emanating from sources other than official coercion"). Whether a statement is coerced is "determined by the totality of the circumstances," *Charlotte E. v. Safir*, 156 F.3d 340, 346-47 (2d Cir. 1998), including "the accused's characteristics," "the conditions of the interrogation," and "the conduct of the police," *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 177, 213 (2d Cir. 2008).

Here, there is no factual support for the claim that Chastain was compelled to tell the agents his Password. The circumstances surrounding Chastain's brief questioning "contain[ed] no traces of the brutality, psychological duress, threats, or unduly prolonged interrogation that courts have previously found when they have concluded that statements were involuntarily made." *United*

States v. Verdugo, 617 F.3d 565, 575-76 (2d Cir. 2010) (collecting cases). Indeed, Chastain's affidavit shows that the agents asked him only a handful of straightforward questions, while he was unrestrained in his own home. The Second Circuit has found un-*Mirandized* statements voluntary in far more coercive environments. *See, e.g.*, *United States v. Siddiqui*, 699 F.3d 690, 706 (2d Cir. 2012) (finding statements not coerced when defendant was questioned while detained, in restraints, and hospitalized because "the defendant was lucid and police conduct was not overbearing"); *Parsad v. Greiner*, 337 F.3d 175, 184-85 (2d Cir. 2003) (finding statement not coerced when defendant was questioned, over the course of hours, in a police station and told the officers he did not want to discuss the crime). Chastain's claim that, after speaking to an attorney, he told the agents that he was not required to provide his Password, *see* Aff. ¶ 9, is of no moment. "[C]oercive police activity is a necessary predicate to holding a [statement] constitutionally involuntary," and Chastain alleged change of heart does not establish any such wrongdoing. *United States v. Haake*, 884 F.3d 400, 409 (2d Cir. 2009).

Accordingly, even if the agents should have read Chastain a *Miranda* warning before asking for his password, the only remedy is barring the Government from using that statement in its case in chief, not going further and suppressing data seized from the iPhone.

III. Chastain's Fourth Amendment Rights Were Not Violated.

Seeking an alternative basis for suppression, Chastain proposes that his Fourth Amendment rights were violated. Specifically, Chastain notes that Agent-1's application for a search warrant said that the warrant did not authorize the Government to "compel Chastain to provide a numeric passcode," and Chastain claims that the agents acted contrary to that representation. Br. 14-16. This argument is wrong on the law because the cases Chastain cites focus on seizing evidence beyond the scope of the search warrant, which is not alleged to have occurred in this case. It is also factually incorrect because Chastain was never compelled to reveal his Password.

"[W]holesale suppression" of evidence seized pursuant to a search warrant is appropriate "only when (1) [the agents] effect a widespread seizure of items that were not within the scope of the warrant,' and (2) do not act in good faith." *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000). "The rationale" for this doctrine is that "Anglo American law" has long had an aversion to "so-called general searches," and "a search that greatly exceeds the bounds of a warrant and is not conducted in good faith is essentially indistinguishable from a general search." *Id.* at 140-41. Accordingly, the test has two separate prongs—a seizure of items outside the scope of the warrant and lack of good faith—both of which must be satisfied before the remedy of wholesale suppression is warranted. *Id.* at 141-42; *see id.* at 142 ("[T]he extreme remedy of blanket suppression should only be imposed in the most extraordinary of cases.").

This doctrine does not provide a legal basis for Chastain's argument. Chastain does not claim that the Government seized data from the iPhone that was outside the scope of the search warrant, much less effected a widespread seizure of such data. There is, then, no relationship between the facts of this case and the concerns about general searches that warrant wholesale suppression in extraordinary cases.

Moreover, as a factual matter, Agent-1's request for the Password was not inconsistent with the terms of the search warrant, let alone so inconsistent as to show a lack of good faith. The search warrant authorized the agents to obtain from Chastain "any physical biometric characteristics" needed to unlock his electronic devices. Ex. B. That portion of the warrant did not prevent the Government from attempting to unlock electronic devices using other means, including by asking Chastain for his passwords. In the application for the warrant, Agent-1 noted that the warrant did not authorize the agents to "*compel* Chastain to provide a numeric passcode,"

id. (emphasis added).[4] But "compel" is not the same thing as "ask." As explained above, compulsion has a specific meaning that requires coercive action by law enforcement, and none of the facts in Chastain's affidavit suggest that the agents in this case used coercive techniques to obtain his Password. *See supra* at 16-17. That has added force in the context of Chastain's Fourth Amendment argument, which requires Chastain to show not only that the agents acted inconsistently with the warrant, but also that they lacked good faith—that is, that they lacked "an objectively reasonable-good faith belief that their conduct [was] lawful." *See United States v. Davis*, 564 U.S. 229, 238 (2011). The facts here provide no grounds to conclude that the agents acted inconsistently with the warrant at all, much less so inconsistent as to lack good faith.

Chastain's Fourth Amendment argument for suppressing the data seized from the iPhone should, accordingly, be rejected.

IV. The Government Inevitably Would Have Accessed The iPhone.

Finally, even if this Court concludes that Chastain's Fourth or Fifth Amendment rights were violated, suppression of data seized from the iPhone is not warranted because the data inevitably would have been discovered, even if Chastain had not given the agents his Password.

"[U]nder the inevitable discovery doctrine," evidence that would otherwise be suppressed "should not be excluded if the government can prove that the evidence would have been obtained inevitably without the constitutional violation." *United States v. Vilar*, 729 F.3d 62, 84 (2d Cir. 2013). To prevail under this doctrine, "the government must prove that each event leading to the discovery of the evidence would have occurred with a sufficiently high degree of confidence for

[4] The statement that the warrant did not authorize the agents to compel Chastain to provide passwords was also not a limitation on the Government's ability to compel the production of passcodes or compel the unlocking of devices through grand jury subpoenas.

the district judge to conclude, by a preponderance of the evidence, that the evidence would inevitably have been discovered." *Id.*

Here, there is no dispute that, even if Chastain did not provide the Password, the Government would have seized the iPhone and attempted to search it pursuant to the search warrant. The only question, then, is whether the Government would have been able to extract the data from the iPhone without the Password. The Government expects that, if this Court held a hearing, the Government inevitably would have been able to extract the data from the iPhone through three separate processes.

First, the Government would have been able to access the iPhone using Chastain's biometric characteristics—specifically, his face. The evidence will show that the iPhone had the "FaceID" features enabled, which means that the iPhone would have unlocked if held in front of Chastain's face. The search warrant authorized the agents to "hold the [iPhone] in front of" Chastain's face to "activate the facial recognition feature," Ex. A, and the agents would have done so had Chastain not provided his password. This would have allowed the FBI to extract from the iPhone the same data that the FBI extracted using the Password, so all of the data Chastain seeks to suppress inevitably would have been seized.

Second, the evidence would show that, even if Chastain did not provide the Password, the agents inevitably would have been able to deliver the iPhone in a "warm" or "after first use" to the FBI team responsible for performing extraction. A device is in a "warm" or "after first use" state if the phone has been turned on, unlocked at least once, and not powered off again since that first unlocking. So long as the iPhone arrived in a "warm" or "after first use" state, the Government would have been able to extract any data from that phone that was not stored on Apple proprietary applications. Because none of the data responsive to the search warrant was stored on such

applications, the Government inevitably would have been able to seize all of the data from the iPhone that Chastain seeks to suppress.

Third, even if the iPhone did not arrive to the FBI extraction team in a "warm" or "after first use" state, the Government would have been able to unlock the iPhone by using a software program to crack the Password. While the amount of time that process would take is uncertain, once the Password was cracked, the Government inevitably would have been able to extract all of the data on the iPhone.

CONCLUSION

Accordingly, the Government respectfully requests that the Court deny Chastain's motions to suppress data seized from the iPhone.

Dated: New York, New York
October 14, 2022

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney

By: /s
Thomas Burnett
Nicolas Roos
Assistant United States Attorneys